CLAIMS

1. A data security system, comprising:

an implicit clearance system;

an explicit clearance system;

a field level clearance system; and

a data anonimization system.

2. The data security system of claim 1, wherein the implicit clearance system comprises a mechanism for setting up a plurality of filters for a set of data, and wherein a user is granted permission to the set of data if the user meets a condition of at least one filter.

3. The data security system of claim 2, wherein the set of data is selected from the group consisting of: a row of data, a data table, and a data field.

4. The data security system of claim 1, wherein the implicit clearance system comprises a table for each filter, wherein each table lists all user ID's that meet the condition of an associated filter.

5. The data security system of claim 1, wherein the explicit clearance system comprises a mechanism for requiring explicit permission to an area of data, and wherein a user is granted permission to the area of data only if explicit permission has been granted.

6. The data security system of claim 5, wherein the area of data is selected from the group consisting of: a row of data, a data table and a data field.

7. The data security system of claim 1, wherein the explicit clearance system comprises:

an explicit areas table that defines all areas of data that require explicit clearance; and

a set of ID tables that define those users who have explicit clearance for each of the areas requiring explicit permission.

8. The data security system of claim 1, wherein the field level clearance system controls access to data types by restricting a user to a predefined view, wherein the predefined view displays a predetermined set of data fields.

9. The data security system of claim 8, wherein the field level clearance system includes a set of data type tables that dictates data types available to each of a plurality of users.

10. The data security system of claim 1, wherein the anonimization system provides a mechanism for replacing a data element in a data record with a unique identifier in order to keep the data record anonymous.

11. The data security system of claim 10, wherein the anonimization system includes:

a reference table for each data field that is to be kept anonymous, wherein each reference table includes a list of anonimized data elements and an associated unique identifier; and

a mechanism for generating a new unique identifier for a data element that does not exist in the list of anonimized data elements.

12. A program product stored on a recordable medium for providing data security, the program product comprising:

means for selectively requiring a user to have explicit permission in order to access a set of data;

means for requiring the user to meet any one of a set of implicit conditions in order access the set of data;

means for limiting access to data records by restricting the user to a predefined view, wherein the predefined view displays a predetermined set of data fields from the data records; and

means for replacing a data element in a data record with a unique identifier in order to create an anonymous data record.

13. The program product of claim 12, wherein the means for selectively requiring a user to have explicit permission comprises:

means for defining all areas of data that require explicit clearance; and

means for defining those users who have explicit clearance for each of the areas requiring explicit permission.

14. The program product of claim 12, wherein the means for requiring the user to meet any one of a set of implicit conditions comprises means for storing a set of acceptable user ID's for each of the implicit conditions.

15. The program product of claim 12, wherein the means for limiting access to a data record includes means for associating each of a plurality of users with one of the predefined views.

16. The program product of claim 12, wherein the means for replacing a data element in a data record with a unique identifier includes:

reference means for each data field that is to be kept anonymous, wherein said reference means includes a list of anonimized data elements and an associated unique identifier; and

means for generating a new unique identifier for a data element that does not exist in the list of anonimized data elements.

17. A method for providing data security, comprising:

selectively replacing data elements in data records with unique identifiers as the data records are being stored in a data warehouse in order to create anonymous data records;

selectively requiring a user to have explicit permission in order to access a set of the data records;

requiring the user to meet any one of a set of implicit conditions in order access the set of the data records if explicit clearance is not required; and

limiting access to data records by restricting the user to a predefined view, wherein the predefined view displays a predetermined set of data fields from the data records.

18. The method of claim 17, wherein the step of selectively requiring a user to have explicit permission comprises:

defining all areas of data that require explicit clearance; and

defining those users who have explicit clearance for each of the areas requiring explicit permission.

19. The method of claim 17, wherein the step of requiring the user to meet any one of a set of implicit conditions includes the step of storing a set of acceptable user ID's for each of the implicit conditions.

20. The method of claim 17, wherein the step of limiting access to a data record includes the step of associating each of a plurality of users with one of the predefined views.

21. The method of claim 17, wherein the step of replacing a data element in a data record with a unique identifier includes:

providing a reference table for each data field that is to be kept anonymous, wherein said reference table includes a list of anonimized data elements and an associated unique identifier; and

generating a new unique identifier for a data element that does not exist in the list of anonimized data elements.